idn brief

abril de 2025

European Deterrence

Deterrence: a New Strategy for the Self-Standing Europe
Pavel Baev

Beyond Resolve: Industrial Capacity and the Credibility of European Deterrence
Nicholas Marsh

Cyber-Warfare and the Logic of Deterrence: How Can Europe Learn from the Ukraine War
Bruno Oliveira Martins

DIRETORA
Isabel Ferreira Nunes
COORDENADOR EDITORIAL
Luís Cunha
CENTRO EDITORIAL
Filipa Teles
PROPRIEDADE, DESIGN GRÁFICO E EDIÇÃO
Instituto da Defesa Nacional

ISSN 2182-5327
Depósito Legal 340906/12

idn Instituto da Defesa Nacional

Calçada das Necessidades, 5, 1399-017 Lisboa
Tel +351 211 544 700
idn.publicacoes@defesa.pt

European Deterrence

Deterrence: a New Strategy for the Self-Standing Europe

Pavel Baev
Research Professor at the Peace Research Institute Oslo (PRIO)

At the start of the fourth year of devastating battles, the long Ukraine War appears to approach a pause, which may not last long – and indeed, may not happen at all, despite the severe exhaustion of the combatants. The "peace deal" envisaged by President Donald Trump and promoted energetically by his administration remains a dubious proposition, which is strikingly different from the commitment by the Western coalition to strive for a durable and just peace "for as long as it takes". Big and small European states are struggling to adjust to this drastic shift of guidelines, and the unprecedented surge of high-level political interactions may signal the emergence of a new resolve to shoulder major responsibility for ensuring collective security. A stable peace could have opened avenues (including in arms control) that would have allowed to engage Russia in designing a new architecture; the unsatisfactory and unjust pseudo-peace that is presently looming guarantees that a new European security system will be built for deterring the Russian threat, hopefully with US contribution but without the familiar leadership. This sadly realistic prospect demands a profound reconfiguration of the deterrence strategy – and urgent research efforts aimed at rethinking its old provisions and assumptions. This reinvention of deterrence is a complex and challenging task, which involves various domains, from nuclear to cyber, connects urgent demands with midterm goals, and accounts for a different exposure to the evolving threat from Russia in several overlapping European sub-regions, from the Arctic to the Eastern Mediterranean. Only several elements of this task can be addressed here, and we can just point out regarding the latter issue that the acute concerns about risks emanating from Russia in the "frontline states", such as Poland, are recognised as legitimate and shared by many countries that are far away from the battlefields in Ukraine, the UK being the key example. For Norway, which has only a short land border with Russia but faces the fast-changing Arctic frontier, it is particularly important to find common ground with Portugal, a state with an informed maritime perspective and strong Atlantic tradition.

Discussions on the new content of deterrence are often reduced to managing the highest risk – preventing a nuclear escalation, and the Ukraine War has certainly focused attention on Russia's vast nuclear arsenal and President Putin's propensity to nuclear brinksmanship. The most alarming part of this old/new "mind game" (which deterrence in essence continues to be) is Russia's big superiority in non-strategic nuclear munitions, and the Europeans have no reasons to assume that the US-Russian talks on strategic stability, which can be resumed if a "peace deal" is indeed negotiated, would address this huge risk to their satisfaction. There is no hard data on the number of Russian non-strategic nuclear weapons and on their compatibility with various tactical and longer-range delivery systems, including the experimental medium-range Oreshnik missile, praised by Putin beyond technical or political reasons. One rational

assumption is, nevertheless, about the impossibility of achieving any kind of numerical parity between the Russian stockpile and a possible European deterrent, comprised of the UK and French nuclear capabilities. Europe will remain interested, therefore, in the continuing deployment of US tactical nuclear weapons in several European states and even in Turkey, controversial as this material part of the "extended deterrence" strategy is certain to be.

In the realm of conventional deterrence, two new questions shape as crucial for the post-war-no-peace security environment: a) How to deter Russia from resuming the aggression against Ukraine? And b) How to deter Russia from testing the European unity by shifting the focus of its attack to another theatre? These questions are closely connected and may, in fact, have one answer: rebuilding the Ukrainian army and military potential. Turning Ukraine into a "steel porcupine" is a task for the midterm, and the immediate decision to deploy a strong European peace-guaranteeing force in Ukraine is perfectly compatible with the investments in rehabilitation and modernisation of its veteran brigades and damaged industries. The "coalition of the willing" is coming together despite the multitude of complications, and even if the US backup will not materialise, ensuring the operational compatibility and interoperability of the European forces with the Ukrainian forces is a feasible task.

Russia is certainly adamantly against any deployment of troops from NATO member states in Ukraine and persists with demands for Ukraine's "demilitarization", but it is not up to Moscow to set conditions for the hypothetic "peace deal". The Trump administration may be willing to accommodate many of Putin's desires, even pre-emptively, but the European stakeholders in the as yet theoretical armistice need to put their security interests first rather than concede to the US decisions. Messaging from Washington, D.C., is clear on the point that the burden of responsibility for guaranteeing the stability of the compromise arrangement will be left for Europe to carry. Ukraine is desperate to get security guarantees, and it may not be immediately obvious that from the European perspective, they work both ways: the European Peace Corps guarantees that Russia is deterred from a new attack on Ukraine, and the Ukrainian "steel porcupine" guarantees that Russia is deterred from shifting the direction of a new attack to the Baltic theatre. The incorporation of Ukraine into the reconfigured and reenergized European security system denies Russia any position of power, whatever effort it may invest in rebuilding its seriously degraded military machine.

The multidimensional and fast-changing domain of unconventional threats, which range from dragging anchors across seabed cables to sophisticated cyber operations, deserves a special examination. Just one point can be made here: Russia is by no means a "hybrid" warfare superpower. Its only advantage in experimenting with sabotage operations of various kinds is in "playing white" (in chess terms) – staging multiple small-scale deniable attacks on the assumption that the adversary would not respond in kind. Offensive moves are indeed far more cost-effective than defensive countermeasures, particularly in the cyber domain. Russia, however, is so vulnerable to different non-military pressures, including sanctions, and lagging so far behind in developing information technologies and IA capabilities that its boldness is inevitably curtailed by high risks of reciprocal measures.

The bottom line is that the security partnership between the EU/NATO Europe and Ukraine maturing into a proto-alliance guarantees the parties a position of strength vis-à-vis the autocratic and war-damaged Russia, even without the US leadership, which presently is on the path of self-undermining and perhaps even self-elimination.

Beyond Resolve: Industrial Capacity and the Credibility of European Deterrence

Nicholas Marsh
Senior Researcher at the Peace Research Institute Oslo (PRIO)

European leaders have warned that there could be war with Russia within a decade. In the absence of a dependable transatlantic security guarantee, European attempts to avoid war with Russia still rely upon deterring Russia by convincing its leadership that any aggression would be met with sufficient force. Yet, European policymakers have not articulated the nature of the war they are preparing for. Drawing on the experience of the Ukraine War, it is plausible that a future conflict between Russia and European NATO members could resemble a protracted war of attrition, rather than a swift, decisive campaign. The Kremlin may calculate that, as has happened in Ukraine, if Russian forces could seize territory in the initial phase, it might then prove very difficult to remove them once the fighting moves to an attritional phase.

To present a credible conventional deterrent, European states must convince Russia that they have the capacity to sustain a long-term war of attrition. If not, the Kremlin may simply calculate the time and losses needed to exhaust NATO members, who would then concede Russian territorial gains. This capacity depends not only upon the personnel needed for large armies, but even more crucially upon a sustained ability to produce vast quantities of arms, ammunition, and other military equipment.

Former Ukrainian Commander in Chief General Zaluzhni (2025) points

out that the ubiquitous presence of drones and electronic warfare has Drones and sensors have allowed the constant surveillance of the battlefield in intimate detail, and drones also account for two-thirds of Russian casualties. These developments mean that troops must remain ensconced in underground defences and an attacker is at an enormous disadvantage. Since 2022, the war of attrition in Ukraine has expended vast quantities of military materiél. The volunteers at Warspotting have verified using video evidence that Russia has lost almost three and a half thousand tanks and seven and a half thousand other types of armoured vehicles. In April 2025, the Ukrainian armed forces estimated that Russia was firing 23,000 artillery shells per day at Ukrainian troops (down from 40,000 before Ukrainian strikes on ammunition depots) (Denisova, 2025). The technology of modern war, which Russian armed forces have implemented much more extensively than their NATO counterparts, may make attrition an inevitable strategy for both sides.

European NATO members can't rely upon outspending Russia. After adjusting for different purchasing power and production costs, both spent equivalent amounts on their armed forces in 2024 (IISS, 2025). In any case, in a war of attrition, industrial capacity is more important than spending. European leaders cannot count on purchasing arms and ammunition from the rest of the world. Ukraine's supporters have already scoured the world for surplus equipment, and it is unclear whether the United States would be willing, or able, to prioritize Europe's needs. Even a cooperative US administration might be constrained by other strategic priorities, such as preparing for war with China. To credibly deter Russia, European states must demonstrate their ability to produce enough munitions independently.

Russia, for its part, has already built up the defence industrial base required to sustain its war of attrition in Ukraine (Danylyuk and Watling, 2025). Though Western sanctions have affected production of advanced systems, Russian firms have adapted supply chains and shifted toward manufacturing equipment that is 'good enough' for the battlefield.

European states still have a window of opportunity to build up their independent industrial capacity, but it may be limited. A Russian attack on a European NATO member may not occur until after fighting in Ukraine has ceased and the Russian armed forces have been reconstituted. In February 2025, the Danish Defence Intelligence Agency (DDIS) warned that, assuming a cessation of fighting in Ukraine and a lack of US aid for its allies, after 5 years Russia would be able to fight another large-scale war in Europe. Similarly, in March 2025, it was reported that the German Federal Intelligence Service (BND) had assessed that Russia was preparing for a major conventional attack against Western Europe, and under similar circumstances, it would be ready to fight a major conventional war against a NATO member by 2030 (Bewarder, Flade and Schmitt, 2025). The countdown to war is uncertain, and Europe may be racing against a clock that it can only glimpse fleetingly.

European rearmament has begun, most notably through an EU initiative, which aims to mobilize around EUR 800 billion in financing. While the plan sets out five-year ambitions, EU officials have cautioned that it might take five to ten years to replace European dependency on the US industry (Foy and Hall, 2025). Even a decade may be optimistic as bottlenecks can delay progress, including through the fragmentation of industries across many countries, a lack of key production capacity, and shortages of trained personnel (Gilli et al., 2025).

The challenges facing European NATO members wanting to deter Russia extend beyond political will, defence spending, or even the size of their armed forces. Time and industrial readiness are crucial variables.Though significant commitments have building credible deterrence may close too soon. If the intelligence estimates are accurate, Russia could be ready to fight before Europe has completed its rearmament. If that were to happen, deterrence would fail not from a lack of resolve, but from an inability to produce the material needed to fight a long war of attrition. Failure to deter Russia might have terrible consequences, not least the prospect of a resort to nuclear weapons if European conventional forces become exhausted.

References

Bewarder, Manuel, Florian Flade and Jörg Schmitt. 2025. 'Plant Moskau den großen Krieg?', Süddeutsche Zeitung, 27 March.

Danish Defence Intelligence Service [Forsvarets Efterretningstjeneste]. 2025. Opdateret vurdering af truslen fra Rusland mod Rigsfællesskabet.

Danylyuk, Oleksandr and Jack Watling. Winning the Industrial War Comparing Russia, Europe and Ukraine, 2022–24, Royal United Services Institute.

Denisova, Kateryna. 2025. 'Ukrainian long-range strikes cut Russia's shell fire rate by nearly half, Syrskyi says', The Kyiv Independent, 9 April.

Foy, Henry and Ben Hall. 2025. 'European military powers work on 5-10-year plan to replace US in Nato', Financial Times, 20 March.

Gilli, Andrea, Mauro Gilli and Niccolò Petrelli. 2025. 'Rearming Europe: Challenges and Constraints', War on the Rocks, 15 April.

International Institute for Strategic Studies (IISS). 2025. 'Global defence spending soars to new high', 12 February. Accessed from https://www.iiss.org/online-analysis/military-balance/2025/02/global-defence-spending-soars-to-new-high /14 April 2025.

Cyber-Warfare and the Logic of Deterrence: How Can Europe Learn from the Ukraine War

Bruno Oliveira Martins
Senior Researcher at the Peace Research Institute Oslo (PRIO)

The introduction of newly developed technologies in the battlefield has been a permanent feat of warfare. Advances in science and technology have always been mobilised to generate advantages in the battlefield and beyond, and the war in Ukraine is not an exception to this rule. Ukraine has become a laboratory for testing new weapons, for the repurposing of dual-use technologies acquired in the civilian market, and for experimenting with the new technological frontiers in the realm of artificial intelligence (AI). The logic of deterrence is challenged by new technologies because they change the rules of the game and, with it, the calculations triggered on the opponent. The Ukrainian laboratory, then, is impacting the way deterrence logics operate not only when it comes to the two belligerent parties, but also in the wider geopolitical arena that the war relates to, specifically Europe. For NATO, the EU, and European countries, conventional means, such as nuclear weapons, large armies, and other military assets, still constitute the main part of its deterrence capabilities. Yet, there are a few factors altering the strategic calculations involved in balancing deterrence in Europe today. These include the United States' disengagement from European security (which fundamentally impacts NATO's deterrence capacity), the use of new technologies with a disruptive potential (such as cyber weapons and mounting levels of AI leading to increasing automation), and the widening of the use of hybrid warfare in countries bordering the active battlefield.

The main claim in this short piece is that these three factors (US disengagement, disruptive technology, and hybrid warfare) bring uncertainty to the current strategic scenario, and uncertainty triggers psychological processes that influence how deterrence operates. This means that the policy and operational measures adopted by European NATO or EU member states to increase deterrence will certainly be influenced by these uncertainties. The first of these factors, US disengagement, is the one that has the greatest impact and that is of most complex management. But it is also the one that gets more attention. For this reason, the remaining of this piece will focus on the other two. It will look at cyberspace as an arena where disruptive technology and hybrid warfare relate to each other and where deterrence logics are being reshaped.

The cyber dimension

Cyberspace is part of NATO's core domain of operations (together with land, sea, air, and space), and this means that the cyber domain is part of NATO's strategic thinking on deterrence. For this reason, several measures have been adopted recently to increase the Alliance's cyber resilience as connected to its deterrent posture. These include the establishment of a Cyberspace Operations Centre in Belgium in 2018 and the adoption of a Comprehensive Cyber Defence Policy in 2021, supporting the alliance's core tasks. At a point when the Ukraine war was already becoming a long-term conflict, the NATO Summit in Washington, D.C., in 2024, created a NATO Integrated Cyber Defence Centre to enhance network protection, situational awareness, and the implementation of cyberspace as an operational domain.

At a more conceptual level, the fact that cyberspace is treated as a core domain for NATO means that NATO is embracing the logic of cross-domain deterrence. This refers to the use of capabilities/assets of one type (say, missiles) to counter threats or combinations of threats of another type (say, nuclear or cyber) in order to prevent attacks. This logic has contact points with the US National Defence Strategy of 2022, which adopted the concept of integrated deterrence, implying an understanding of deterrence as mobilising all assets of all types across all partnerships to exert deterrent power on adversaries. This context provides an important background for European security responses post-2022. The war in Ukraine has exhibited a combination of conventional war (e.g. large armies, trenches, land invasion, fight across all domains) with elements of high-tech war (e.g. multiple types of drones, increasing levels of automation in decision-support systems) and hybrid warfare in third countries (e.g. misinformation, election interference, cyber-attacks on critical infrastructure). Likewise, Europe's deterrence capacity will have to be cross-sectoral and its ability to preempt adversarial attacks will largely depend on its capabilities in different domains. And even though the cyber domain has played a smaller role in the war than many anticipated, it has nevertheless been an important part of the conflict. Russia conducted several attacks in the run-up to the invasion and in the subsequent weeks, but their efficiency was not as envisaged. This led to a shift in Russia's strategy away from large direct attacks on the front line and to critical infrastructure toward intelligence gathering, target acquisition, and some specific operations, but still away from the large cyber conflict that seemed poised to happen.

Another important lesson for Europe deals with how AI is impacting the logic of deterrence. The growing reliance on (semi)autonomous warfare reduces human intervention in decision-making processes, and this impacts the logic of deterrence, which relies widely (although not exclusively) on psychological dimensions that can only be associated with humans. AI will have important implications on how actors deal with the unknown. The use of AI

across different operational domains (warfare, decision support systems, foresight) and in different scientific domains (biotechnology, chemistry, new materials) brings enormous uncertainty and may lead to logics of escalation. For this reason, developing strategies to manage uncertainty (e.g. pushes for AI regulation, norm-making, new routines) may prove crucial to managing the undesired consequences of AI.

Moreover, the use of AI in the cyber domain is rapidly becoming a source of misinformation in Europe, which is only likely to grow. Hybrid warfare strategies rely heavily on misinformation, disinformation, and psychological elements to produce intended results. European strategies to reinforce the continent's deterrence and resilient power need to further combat AI-based hybrid warfare.

In 2025, the logic of deterrence has grown into a cross-domain issue that requires a wide set of measures to remain effective in the face of multiple challenges. Since 2022, the Ukraine war has acted as an accelerator of some pre-existing dynamics, and Europe's attempt to build a credible deterrent to potential adversarial attacks is increasingly based on lessons learned from the conflict.